AN12048

Safety application note for MC33904 and MC33905

Rev. 1.0 — 21 September 2017 Application note

Document information

Information	Content
Keywords	AN12048, safety, MC33904, MC33905
Abstract	This document discusses the safety requirements for the use of an NXP product and in functional safety relevant applications requiring high functional safety integrity levels.

1 Introduction

MC33904 and MC33905 were developed in 2009, two years before the release of ISO 26262. The devices have not been developed following ISO 26262 processes and have not been assessed for an ASIL level. The devices can be used in applications targeting certain levels of ASIL. This document shows how to use and implement the device to target functional safety applications.

This document discusses requirements for the use of the MC33904 and MC33905 system basis chip (SBC) family in functional-safety relevant applications requiring functional safety integrity levels. It is intended to support system and software engineers who are taking advantage of the MC33904 and MC33905 features, as well as achieving additional diagnostic coverage by software measures.

Several measures are prescribed as safety requirements whereby the measure described is assumed to be in place when analyzing the functional safety of this system basis chip. In this sense, requirements in the safety application note are driven by assumptions [SMR_xx] concerning the functional safety of the system integrating the MC33904 and MC33905 devices.

- **Assumption:** An assumption being relevant for functional safety in the specific application under consideration (condition of use). It is assumed the user fulfills an assumption in the design.

For the use of the system basis chip, means if a specific safety manual assumption is not fulfilled, it has to be rationalized that an alternative implementation is at least similarly efficient concerning the functional safety requirement in question. For example, the alternative provides the same coverage, reduces the likelihood of common mode failure (CMF), and so on. Or, the estimation of an increased failure rate (λSPF, λRF, λMPF, λDU, etc.) and reduced metrics (SFF: safe failure fraction, SPFM: single-point fault metrics, LFM: latent fault metric) due to the deviation are specified.

This document also contains guidelines describing how to configure and operate the MC33904 and MC33905 for functional-safety relevant applications requiring high functional safety integrity levels. These guidelines are preceded by one of the following text statements:

- **Recommendation:** This is either a proposal for the implementation of an assumption or a reasonable measure that is recommended to be applied, if there is no assumption in place. The user has the choice whether to follow the recommendation or not.
- **Rationale:** This is the motivation for a specific assumption and/or recommendation.
- **Implementation hint:** This gives specific hints on the implementation of an assumption and/or recommendation on the MC33904 and MC33905. The user has the choice whether to follow the implementation hint or not.

These guidelines are considered to be useful approaches for the specific topics under discussion. The user needs to use discretion in deciding whether these measures are appropriate for the intended applications.

This document is valid only under the assumption that the system basis chip is used in functional safety applications requiring a fail-indicate system basis chip. A fail-operational mode of the MC33904 and MC33905 is not described.

This document targets functional safety integrity levels. For functional safety goals that do not require functional safety integrity levels, system integrators need to tailor the requirements for the intended application.

1.1 Customer task responsibility

In a context of customer applications, this is a list of required customer tasks under the responsibility of those customers. The list is delivered as an example and is not exhaustive. In case of questions, the customer should contact a local NXP representative.

- Use of the latest revision of MC33904 and MC33905 documentation. This includes, but is not limited to data sheets, user guides, safety application notes, FMEDAs, application notes, errata, and others.
- Other or additional safety requirements, such as IEC 61508 or IEC 61784, might have to be considered depending of the target application and required standard.
- Verify that the application mission profile is well covered by the MC33904 and MC33905 devices as showed in Table 1.
- Compare system requirements versus MC33904 and MC33905 requirements and make sure there are no deviances.
- • Establish validity of assumptions at the system level considered in Section 2 "Assumptions of use".
  - Verify that the fault tolerant time interval (FTTI) of the MC33904 and MC33905 is under the system FTTI requirement, regardless of the fault type.
  - Verify the violation of the technical assumptions as described in Section 2.6 "Technical safety requirements".
  - Verify the safe state considerations described in Section 2.4 "Safe state".
- Consider assumptions, such as typical mission profile and failure rate data book (IEC 62380).
- During safety analysis, the nonfunctional blocks, such as debug, should also be considered.
- Perform calculations and verify the safety metrics.
- Perform DFA analysis.
- Validate MC33904 and MC33905 outputs behave as expected in the application, and also during error conditions.
- Consider and verify single-point failures and latent failures at the system level.
- Consider and verify systematic errors during development.
- Verify the effectiveness of diagnostics at the system level.
- Perform fault injection tests and validate safety mechanisms.
- Consider all recommendations and implementation hints given in this safety manual.

1.2 Safety documentation set

This sections lists helpful documentation for the user.

Document number	Document type	Description
ISO 26262	Standard	ISO 26262 Road vehicles - Functional safety, November 2011
IEC TR 62380	Standard	Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment
MC3390x	Data sheet	SBC Gen2 with CAN high speed and LIN interface data sheet
doc_MC33904_5_Dynamic_FMEDA	Dynamic FMEDA	Failure Mode Effects and Diagnostic Analysis Document.

Document number	Document type	Description
201632088A	PPAP	Report summarizing data gathered during qualification of the MC33904 and MC33905 following AECQ100-RevG requirements.
AN4770	Application note	Implementing the MC33903/4/5 CAN and LIN system basis chip

1.3 Vocabulary

For the purposes of this document, the vocabulary defined in ISO 26262-1 apply to this document.

Specifically, the following terms apply.

- **System:** Functional safety-related system implementing the required functional safety goals necessary to achieve or maintain a safe $state_{system}$ for the equipment under control (control system). The system is intended to achieve on its own or with other electrical/electronic/programmable electronic functional safety-related systems, the necessary functional safety integrity for the required safety functions.
- **System integrator:** The person responsible for the system integration.
- **Element:** Part of a subsystem comprising of a single component or any group of components (for example, hardware, software, hardware parts, software units) performing one or more element safety functions (functional safety requirements).
- **Trip time:** The maximum time of operation of the SBC without switching to a power-down state.

1.4 Faults and failures definition

Failures are the main impairment to functional safety:

- **Systematic failure:** A failure manifested in a deterministic way to a certain cause (systematic fault) that can only be eliminated by a change of the design process, manufacturing process, operational procedures, documentation, or other relevant factors. Thus, measures against systematic faults are reductions of systematic faults, such as implementing and following adequate processes.
- **Random hardware failure:** A failure that can occur unpredictably during the lifetime of a hardware element and follows a probability distribution. Thus, measures reducing the likelihood of random hardware faults are either the detection and control of the faults during the lifetime, or reduction of failure rates. A random hardware failure is caused by either a permanent fault, such as physical damage, an intermittent fault, or a transient fault. Permanent faults are unrecoverable. Intermittent faults are for example, faults linked to specific operating conditions or noise. Transient faults are, for example, EMI radiation. An affected configuration register can be recovered by setting the desired value or by a power cycle. Due to a transient fault, an element may be switched into a self-destructive state (for example, single event latch up), and therefore may cause permanent destruction.

1.4.1 Faults

The following random faults may generate failures, which may lead to the violation of a functional safety goal. Citations are according to ISO 26262-1. Random hardware faults occur at random times, which results from one or more of the possible degradation mechanisms in the hardware.

- **Single-point fault (SPF):** A fault in an element not covered by a safety mechanism that results in a single-point failure and leads directly to the violation of a safety goal. Figure 1(a) shows an SPF inside an element generating a wrong output.
- **Latent fault (LF):** A multiple-point fault whose presence is not detected by a safety mechanism nor perceived by the driver. An LF is a fault that does not violate the functional safety goal(s) itself, but leads in combination with at least one additional independent fault to a dual- or multiple-point failure, which then leads directly to the violation of a functional safety goal. Figure 1(b) shows an LF inside an element, which still generates a correct output.
- **Residual fault (RF):** A portion of a fault that, by itself, leads to the violation of a safety goal, where the portion of the fault is not covered by a functional safety mechanism. Figure 1(c) shows an RF inside an element; which, although a functional safety mechanism is set in place, generates a wrong output, as this particular fault is not covered by the functional safety mechanism.
- **Dual-point fault (DPF):** An individual fault that, in combination with another independent fault, leads to a dual-point failure, which leads directly to the violation of a goal. Figure 1(d) shows two LFs inside an element generating a wrong output.
- **Multiple-point fault (MPF):** An individual fault that, in combination with other independent faults, leads to a multiple-point failure, which leads directly to the violation of a functional safety goal. Multiple-point faults are not covered.
- **Safe Fault (SF):** A fault whose occurrence does not significantly increase the probability of violation of a safety goal. Safe faults are not covered in this document. Single-point faults, residual faults, or dual-point faults are not safe faults.

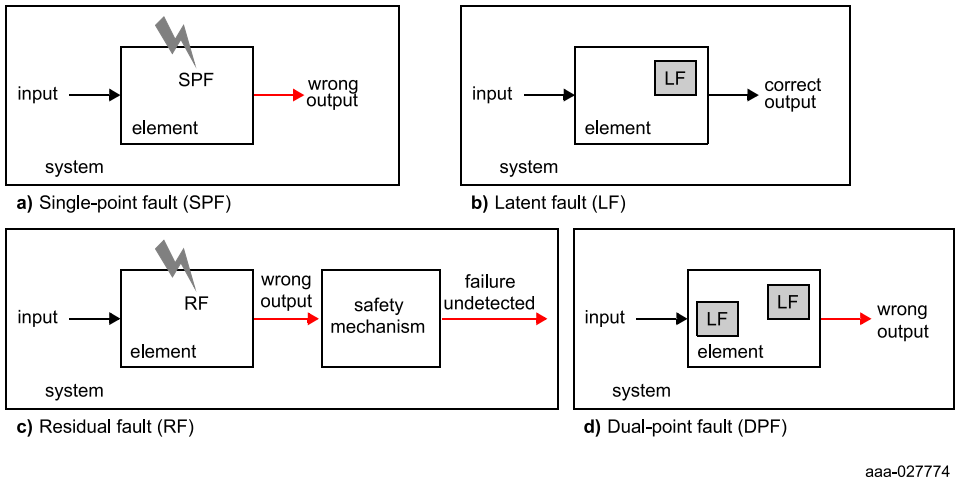

Figure 1. Faults

SPFs must be detected within the FTTI. Latent faults (dual-point faults) must be detected within the MPFDI. In automotive applications, MPFDI is generally accepted to be once per typical automotive trip time (t_{TRIP}) by test routines. For example, BIST after power-up is acceptable. This reduces the accumulation time of latent faults from the lifetime of the product t_{LIFE} to t_{TRIP}.

Table 1 lists a profile with a typical trip time for automotive applications.

1.4.2 Failures

- **Common cause failure (CCF):** CCF is a coincidence of random failure states of two or more elements in separate channels of a redundancy element, leading to the defined

element failing to perform its intended safety function, resulting from a single event or root cause, such as chance cause, nonassignable cause, noise, or natural pattern. Common cause failure causes the probability of multiple channels (N) having a failure rate to be larger than $\lambda_{single\ channel}^{N}$ ($\lambda_{redundant\ element} > \lambda_{single\ channel}^{N}$).

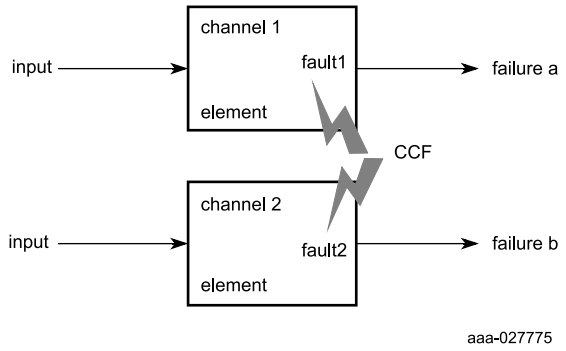

Figure 2. Common cause failures

- **Common mode failure (CMF):** CMF is a subset of CCF. A single root cause leads to similar coincidental erroneous behavior (with respect to the safety function) of two or more (not necessarily identical) elements in redundant channels, resulting in the inability to detect the failures. Figure 3 shows three elements within two redundant channels. One single root cause (CMF A or CMF B) leads to undetected failures in the primary channel and in one of the elements of the redundant channel.

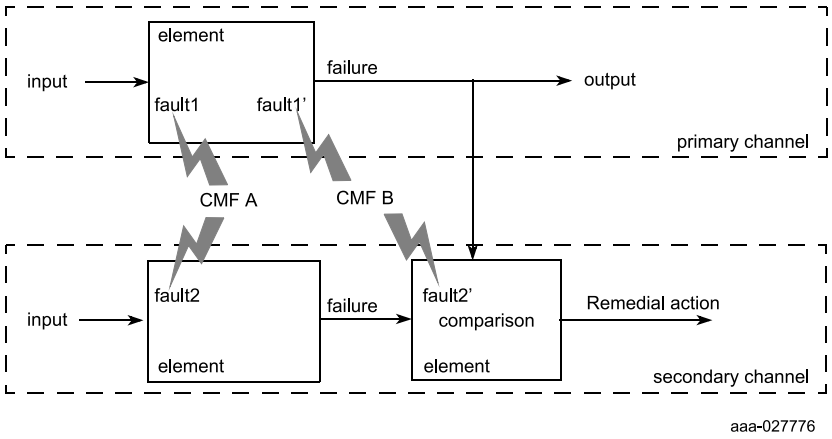

Figure 3. Common mode failures

- **Cascaded failure (CF):** CFs occur when local faults of an element in a system ripple through interconnected elements causing another element or elements of the same system and within the same channel to fail. Cascading failures are dependent failures, not common cause failures. Figure 4 shows two elements within a single channel, to which a single root cause leads to a fault (fault 1) in one element resulting in a failure (failure a), and causing a second fault (fault 2) within the second element (failure b).

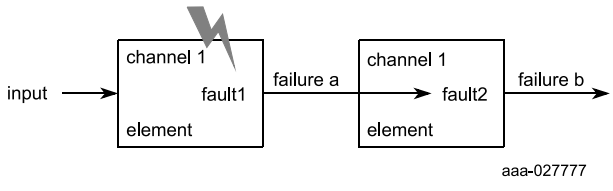

Figure 4. Cascading failures

2 Assumptions of use

The part numbers supported by this safety manual are from the MC33904 and MC33905 families.

2.1 Generic safety system architecture

MC33904 and MC33905 are designed to be used in automotive or industrial applications which are needed to fulfill functional safety requirements, as defined by functional safety integrity levels, such as ASIL B of ISO 26262.

Figure 5 shows a generic safety system architecture example. MC33904 and MC33905 are intended to be the main power supplies for the MCU (V_{DD}), with MCU monitoring (watchdog) and Fail-safe outputs (SAFE) to put the system in safe state.

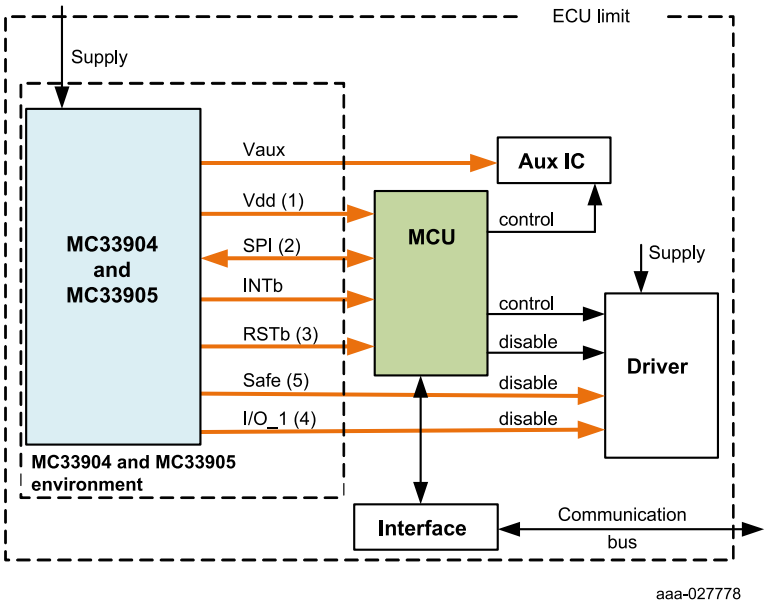

Figure 5. Generic safety system architecture

- V_{DD} (1): MCU core supply (safety related function)
- SPI (2): Serial peripheral Interface between MCU and MC33904 or MC33905 used for watchdog (safety monitoring)
- RSTB (3): Active low bidirectional reset (not safety)
- IO_1 (4): Safe activation in case of Overvoltage on V_{DD}
- Safe (5): Fail-safe output (safety related function)

2.2 Operation of use and mission profile

MC33904 and MC33905 can be used to target an ASIL-B level of safety integrity when applying all recommendations and applicability of the system assumptions mentioned in this safety manual and for the mission profile of typical safety automotive applications.

Assumption: [SMR_01] It is assumed MC33904 and MC33905 are used in 12-volt automotive applications for which the battery voltage, for example pin VSUP1, VSUP2, and VSENSE, never exceeds the maximum ratings of the MC33904 and MC33905.

Above this voltage, the MC33904 and MC33905 run the risk of being destroyed and the safety requirements are no longer satisfied.

Assumption: [SMR_02] It is assumed MC33904 and MC33905 are used in applications for which the fault tolerant time interval is ≥ 256 ms. A shorter fault tolerant time interval must be deeply analyzed. This time interval can be reduced to 100 ms.

Assumption: [SMR_03] It is assumed MC33904 and MC33905 are used in applications for which the mission profile is equivalent to or less aggressive. See Table 1.

Assumption: [SMR_04] It is assumed when the multiple-point fault time interval is ≤ 12 hours, then the driving cycle is ≤ 12 hours.

Assumption: [SMR_05] It is assumed the normal operating range of MC33904 and MC33905 is fulfilled by the compliance to the MC33904 and MC33905 data sheet.

Assumption: [SMR_06] To avoid systematic errors during system integration, it is the system integrator's responsibility to follow NXP recommendations as described in the MC33904 and MC33905 data sheet and application note available at www.nxp.com.

Assumption: [SMR_07] It is the system integrator's responsibility to report all field failures of the devices to the silicon supplier.

Rationale: To cover the ISO 26262-7 (6.5.4) and ISO 26262-7 (6.4.2.1).

Table 1. Temperature profile for mission profiles

Temperature (°C)	TJ (°C)	Operating time in a year (Hours)	Ton/Toff (%)
12.5	32.5	2.2	0.03
17.5	37.5	2.2	0.03
22.5	42.5	30.7	0.35
27.5	47.5	30.7	0.35
32.5	52.5	477.4	5.45
37.5	57.5	477.4	5.45
42.5	62.5	1070.9	12.23
47.5	67.5	1070.9	12.23
52.5	72.5	1539.6	17.58
57.5	77.5	1539.6	17.58
62.5	82.5	965.8	11.03
67.5	87.5	965.8	11.03
72.5	92.5	286.9	3.28
77.5	97.5	286.9	3.28
82.5	102.5	2.2	0.03
87.5	107.5	2.2	0.03
	Time ON	8751	99.9

Note: *The product is always powered on in the cycle.*

Two starts of the vehicle during night and four during day for 335 days in the year are considered.

The ambient temperature considered is outside the module. An increase of die temperature of 20 °C versus outside, based on customer information (power dissipation and thermal resistance) are considered.

2.3 Safety integrated level

Table 2. Safety integrated level

Safety related function	Target System ASIL level
MC33904 and MC33905 must provide V_{DD} supplies within the specified voltage range	ASIL B
MC33904 and MC33905 must perform a periodic handshake (watchdog) in order to confirm the correct behavior of the MCU	ASIL B
MC33904 and MC33905 must indicate a Fail-safe state by virtue of the FS0B output within the FTTI time	ASIL B

2.4 Safe state

A safe state of the system is named safe $state_{system}$ whereas a safe state of the MC33904 and MC33905 is named safe $state_{SBC}$. A safe $state_{system}$ of a system is an operating mode without an unreasonable probability of occurrence of physical injury or damage to the health of people. A safe $state_{system}$ may be the intended operating mode or a mode where the system has been disabled.

Likewise, a safe $state_{SBC}$ of the MC33904 and MC33905 is by definition one of following operation modes, see Figure 6:

- Operating correctly
  - Outputs depend on application
    - Explicitly indicating an error (safe $state_{SBC}$)
  - Fail-safe outputs SAFE indicating an error (active-low)
    - Completely unpowered

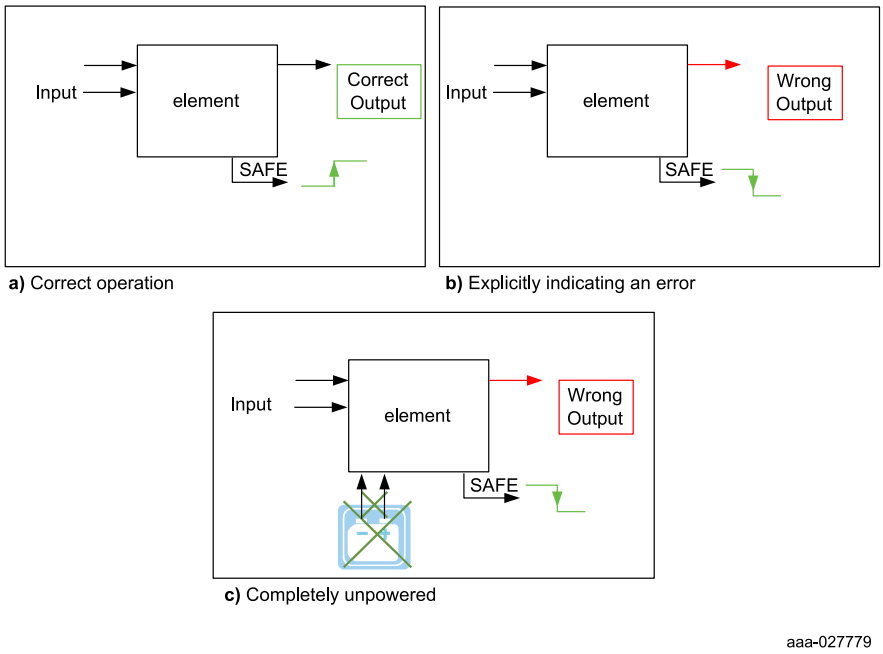

Figure 6. Safe state$_{SBC}$ of the MC33904 and MC33905

Assumption: [SMR_08] It is the system integrator's responsibility to ensure the system transitions itself to a safe state$_{system}$ when the MC33904 and MC33905 explicitly indicates an error via its Fail-safe outputs (SAFE).

Assumption: [SMR_09] It is the system integrator's responsibility to ensure the system transitions itself to a safe state$_{system}$ when the MC33904 and MC33905 are completely unpowered.

MC33904 and MC33905 have two main SAFE states, mode A and mode B. In each of them, the SAFE pin is asserted low. Differentiation between the SAFE state A and B is the V_{DD} remaining ON or being turned OFF. As extra option the V_{DD} turn off can be controlled by external conditions (sub STATE, B1, B2, and B3).

Table 3. Fail safe options

Resistor at DBG pin	SPI coding - register INIT MISC bits [2,1,0] (higher priority that Resistor coding)	Safe mode code	V_{DD} status
< 6.0 k	bits [2,1,0) = [111]: verification enable: resistor at DBG pin is typ 0 kΩ (RA) - Selection of SAFE mode A	A	Remains ON
typ 15 k	bits [2,1,0) = [110]: verification enable: resistor at DBG pin is typ 15 kΩ (RB1) - Selection of SAFE mode B1	B1	Turn OFF 8 s after CAN traffic bus idle detection.
typ 33 k	bits [2,1,0) = [101]: verification enable: resistor at DBG pin is typ 33 kΩ (RB2 - Selection of SAFE mode B2	B2	Turn OFF when I/O_1 low level detected.
typ 68 k	bits [2,1,0) = [100]: verification enable: resistor at DBG pin is typ 68 kΩ (RB3) - Selection of SAFE mode B3	B3	Turn OFF 8 s after CAN traffic bus idle detection AND when I/O_1 low level detected.

2.5 Single-point fault tolerant time interval

The single-point fault tolerant time interval (FTTI) is the time span between a failure having the potential to give rise to a hazardous event, and the time by which counteraction has to be completed to prevent the hazardous event from occurring. It is used to define the sum of the worse case fault indication time and the time for execution of corresponding countermeasures (reaction). Figure 7 shows the FTTI for a single-point fault occurring in the SBC.

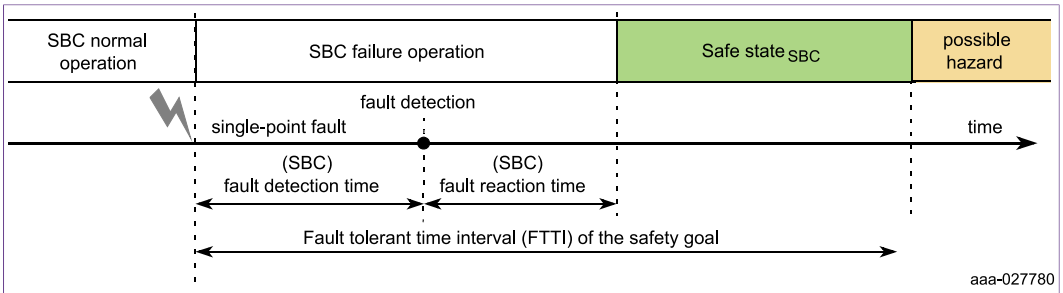

Figure 7. Fault tolerant time interval for single-point faults

Fault indication time (Fault detection time + Fault reaction time) is the time it takes from the occurrence of a fault to switching into safe $state_{SBC}$, for example, indication of the failure by asserting the Fail-safe output pin.

Switching into safe $state_{SBC}$ must occurs within the FTTI. Three events should switch the device in safe $state_{SBC}$ or safe $state_{SYSTEM}$:

- **V_{DD} undervoltage:** Fault indication is 40 µs (safe $state_{SBC}$)
- **WD failure:** longest fault indication is by default 256 ms (safe $state_{SBC}$)
- **Reset shorted to ground:** Fault indication is 100 ms (safe $state_{SBC}$)
- **V_{DD} overvoltage (V_{DD} + 1.5 V):** (safe $state_{SYSTEM}$)

Therefore, by default, FTTI is 256 ms, which is the WD refresh window. FTTI can be reduced to 100 ms, setting the WD refresh window to a lower duration (< 100 ms). Then FTTI is now 100 ms, which is a fault indication time of a reset shorted to ground failure.

2.6 Technical safety requirements

List of the assumed technical safety requirements **[TSR_xx]** of the element considered as potentially violating the safety goals.

Assumption: [TSR_01] It is assumed the MC33904 and MC33905 are used in combination with other devices in the application (i.e. MCU, other analog IC).

Assumption: [TSR_02] It is assumed an out of range operation of the power management integrated circuit (V_{DD}) is considered a violation of at least one of the safety goals of the system.

Assumption: [TSR_03] It is assumed the MC33904 and MC33905 provide the safety mechanism for undervoltage monitoring of the power management integrated circuit. When the monitoring detects a fault, it activates the safe $state_{SBC}$ (SAFE output active low) within the FTTI.

Assumption: [TSR_04] Faults having a direct impact on violation of TSR03 are assumed as single point faults.

Assumption: [TSR_05] It is assumed an abnormal SW and HW execution of the MCU is considered a violation of at least one of the safety goals of the system.

Assumption: [TSR_06] It is assumed the MC33904 and MC33905 provide the safety mechanism for temporal and logical monitoring (watchdog) of an MCU. When the monitoring detects a fault, it activates the safe $state_{SBC}$ within the FTTI.

Assumption: [TSR_07] Faults having a direct impact on the violation of TSR06 are assumed as latent faults.

3 Failure rates and FMEDA

3.1 Failure handling

Failure handling can be split into two categories:

- Failure handling before enabling the system level safety function. For example, during or following the MCU initialization. These errors are required to be handled before the system enables the safety function, or in a time shorter than the respective FTTI after enabling the safety function.
- Failure handling during runtime with repetitive supervision while the safety function is enabled. These errors have to be handled in a time shorter than the respective FTTI.

Assumption: [SMR_10] It is assumed single-point and latent fault diagnostic measures complete operations, including fault reaction, in a time shorter than the respective FTTI when the safety function is enabled.[END]

Recommendation: It is recommended to identify startup failures before enabling system level safety functions.

A typical failure reaction regarding power-up/start-up diagnostic measures is not to initialize and start the safety function, but instead to provide failure indication to the operator/user.

3.2 Failure rates

The MC33904 and MC33905 failure rate data is derived from the IEC/TR 62380, to quantify the hardware architectural metrics for the evaluation of the effectiveness of the design architecture against the requirements for random hardware failures handling.

The random hardware failures addressed by these metrics are limited to some of the item's safety-related electrical and electronic hardware parts, namely those which can significantly contribute to the violation or the achievement of the safety goal, and to the single-point, residual, and latent faults for those parts. Only the electrical failure modes and failure rates are considered for the MC33904 and MC33905.

The IEC/TR 62380 considers the failure rate model for permanent faults in a semiconductor device to be the sum of three subcomponents:

- The **Die** predictive failure rate (46.61 FIT), which depends mainly on
  - Silicon parameters, such as the technology and its maturity and the number of transistors
  - Application parameters like the mission profile, the power dissipation and the junction to ambient thermal resistance
- The **Package** predictive failure rate (25.38 FIT), which depends mainly on

  - Package parameters, such as the number of pins, the pitch
  - Application parameters, such as the mission profile, the temperature cycles, the board material
- The **Interface electrical overstress** predictive failure rate (0 FIT)

The total device failure rate is **72 FIT**.

The transient faults are not considered for MC33904 and MC33905 developed in 0.25 µm technology without SRAM. The only potential concern for soft errors would be in logic latches and flops. Logic soft error upsets are simply not a significant risk at this size nodes, due to higher voltage and capacitance, making it very difficult to cause an upset by radiation.

The method used to evaluate and to quantify the hardware architectural metrics is based on the FMEDA, which details the determination of error causes and their impact on the system. The hardware architectural metrics are dependent upon the context of use of the MC33904 and MC33905:

- Mission profile of the application in which the MC33904 and MC33905 are operating
- Selection/usage of the functions and functional safety mechanisms implemented in the application

3.3 FMEDA overview

MC33904 and MC33905 were developed before the introduction of the ISO 26262 standard. However, a functional safety failure analysis on the hardware design was performed to identify failure causes and their effects and quantitative safety metric values.

FMEDA inductive analysis was the method applied. This FMEDA is based on spreadsheets with the capability to enable safety analysis of the MC33904 and MC33905 features implemented for a specific application.

The MC33904 and MC33905 FMEDA sheet is an example only, based on the result of the safety analysis performed for the context of use of the MC33904 and MC33905, using the mission profile described in Table 1, and when applying all recommendations and assumptions mentioned in this safety manual.

Assumption: [SMR_11] It is assumed simultaneous pin disconnections (i.e. pin lift on the PCB) are restricted to 1 during pin FMEA and FMEDA analysis.[END]

Assumption: [SMR_12] It is assumed the thermal connection of the exposed pad to the PCB is always ensured due to its large size.[END]

Assumption: [SMR_13] Short-circuit between PCB tracks is not considered.[END]

Assumption: [SMR_14] External component disconnection is not considered.[END]

In a context of customer applications, the FMEDA example provided by NXP must be customized to fit for the application requirements. The final customized FMEDA is under the responsibility of the customer, and then solely responsible for the safety metric values.

The MC33904 and MC33905 FMEDA document associated with the MC33904 and MC33905 failure rate estimation document is available upon request, when covered by a NXP Semiconductors NDA. Contact your local NXP representative.

4 Functional safety concept

4.1 Hardware requirements at the system level

This section lists necessary or recommended measures on the system level for the MC33904 and MC33905 to achieve the functional system safety goal(s).

The MC33904 and MC33905 offer an integrated functional safety architecture, and other items to detect faults. By these means, single-point failures and latent failure can be detected with a high diagnostic coverage.

However, not all failure modes may be detected on a complete system by the MC33904 and MC33905, so it is assumed a separate circuitry is used to bring the system into the safe state$_{system}$ (MCU) in such cases.

Figure 8 depicts the functional safety related elements of the MC33904 and MC33905.

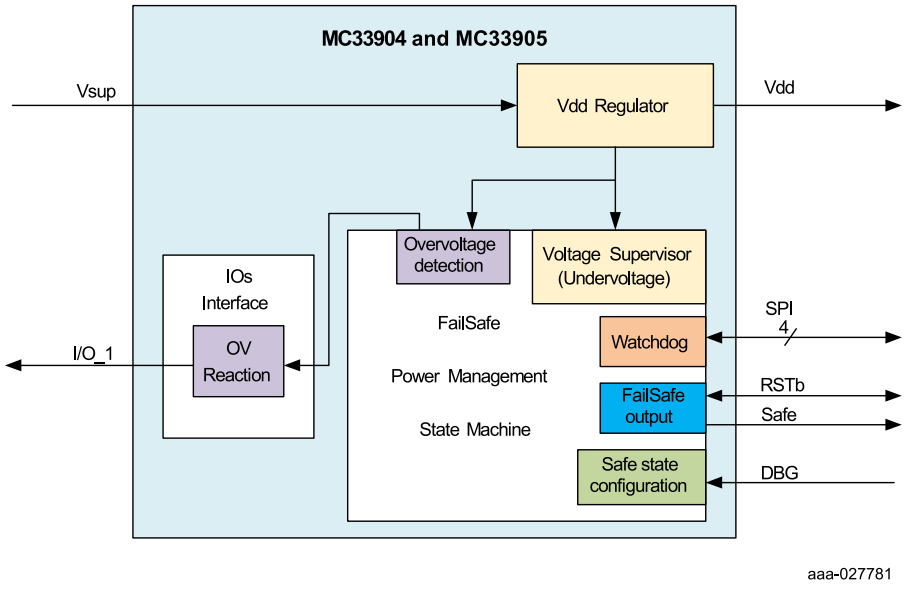

Figure 8. MC33904 and MC33905 functional safety blocks

- V_{DD} is a voltage linear regulator. It is dedicated to the MCU core supply (with 3.3 V or 5.0 V), selectable with part number differentiation.
- The DEBUG pin is used to configure the Fail Safe mode operation.
- SAFE pin is asserted low to put device in safe state$_{SBC}$
- IO_1 can be used in addition to Safe pin to put the system in Safe state when V_{DD} overvoltage is detected.
- Watchdog is part of the safety mechanism to check MCU functioning

Figure 9 depicts a simplified application schematic for a functional safety relevant application in conjunction with an MCU (only functional safety-related elements shown). The MC33904 and MC33905 supply the MCU with the required supply voltages (3.3 V or 5.0 V). Voltages generated by the MC33904 and MC33905 are monitored for undervoltage by the embedded voltage supervision.

Via the SPI communication interface, the MC33904 and MC33905 repetitively trigger the watchdog from the MCU with a valid answer. A dedicated Fail-safe state machine is

implemented to bring and maintain the application in safe $state_{system}$. During a failure, such as a V_{DD} undervoltage, RSTB and/or SAFE are asserted low.

- The reset pin (RTSB) of the MC33904 and MC33905 controls and monitors the reset pin of the MCU.
- A Fail-safe output (SAFE) is available to control or deactivate any Fail-safe circuitry, such as a power switch, in redundancy with the MCU.
- A GPIO output (IO_1) is available to control or deactivate any Fail-safe circuitry in case of V_{DD} overvoltage.

An interrupt output (INTB) for error information is connected to the NMI input of the MCU.

By a connection of the signal MUX_OUT to an ADC-input of MCU, further diagnostic measures are possible, such as reading temperature or measuring V_{BATT}. Additionally, the MC33904 and MC33905 may act as a physical interface to connect the MCU directly with a CAN or LIN bus.

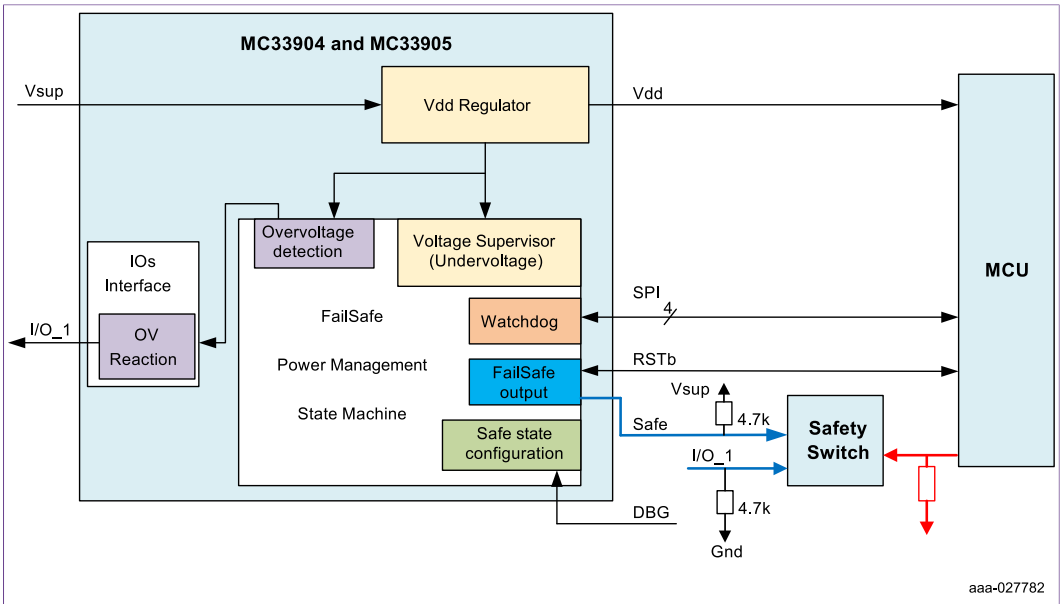

Figure 9. Functional safety-related connection to the MCU

5 Safety interoperation with MCU

This section describes safety interoperation with MC33904 and MC33905 and MCU for applications requiring high functional safety integrity levels. Failure rates of external devices have to be included in the system FMEDA by the system integrator.

5.1 Power supply

5.1.1 V_{DD}

The MC33904 and MC33905 provide a dedicated voltage supply rail for the main input voltage of the MCU, or directly for the core of the MCU, such as the V_{DD}.

The voltage level of V_{DD} supply is selectable by part number. The accuracy of VDD is ±2.0 %.

This supply voltage must be in the specified operating range of the MCU, because an overvoltage might cause permanent damage to the MCU. It is therefore either required to de-energize the MCU or to decommission/replace the MCU after an overvoltage event. An undervoltage might lead to an unexpected behavior of the MCU.

Recommendation: It is recommended at the system level to avoid V_{DD} overvoltage and/or undervoltage, or to permanently disable (safe $state_{system}$) the system in the event of an overvoltage/undervoltage.

Rationale: To ensure overall operation of the MCU according to its data sheet.

Implementation hint: The MC33904 and MC33905 provide an undervoltage monitoring of the V_{DD}. If the V_{DD} is below the value specified in the MC33904 and MC33905 data sheet, the MCU is kept powerless by switching off V_{DD}, such as mode SAFE B, and the SBC switches the system to a safe $state_{system}$ within the FTTI and maintains safe $state_{system}$ through Fail-safe outputs (SAFE).

5.2 Safety output – SAFE

The safety output is used to switch the system to the Fail-safe state (safe $state_{system}$). The SAFE output structure is an open drain.

5.2.1 SAFE

SAFE is a dedicated, active, low signal integrated in the MC33904 and MC33905 to bring the system to the Fail-safe state (safe statesystem) when needed. This safety output can be used for opening the power supply line or disabling the half-bridge drive of a motor/valve or activating another safety mechanism.

Assumption: [SMR_15] An output in high-impedance is not considered safe at the system level. It is the system integrator's responsibility to make sure external components connected to SAFE are available to bring the safety critical outputs to a known level during operation. [END]

Rationale: To bring the functional safety-critical outputs to a defined voltage level at anytime.

Implementation hint: An external pull-up resistor must be connected to the right voltage rail, up to battery voltage.

Assumption: [SMR_16] It is the system integrator's responsibility to ensure opening the safety switch in a system must not be driven by the SAFE only, but also by the MCU or I/O_1.[END]

Rationale: To have a redundant path to cover an external SAFE short to high failure mode.

Implementation hint: A redundant signal coming from the MCU (in red) with a pull-down resistor to cover passive state when the MCU is in reset or SAFE coming from MC33904 and MC33905 (in blue).

Figure 14 shows the connection to ensure good safety operation of SAFE.

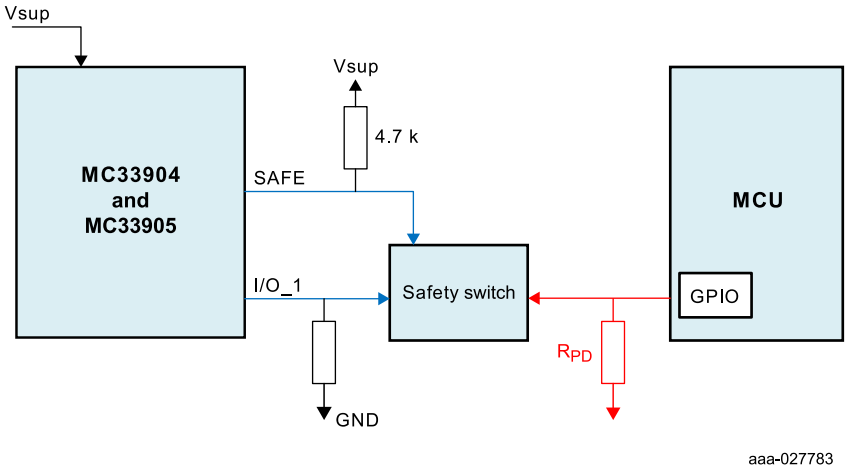

Figure 10. External components on SAFE and redundant safety path from the MCU

5.2.2 Release of SAFE

When the Fail-safe output SAFE is asserted low by the device due to a fault, some conditions must be validated before allowing these pins to be released by the device. The conditions to leave the safe state$_{SBC}$ are:

- The fault is removed.
- Proper read and clear of the SPI flags reporting the SAFE conditions.

Release of SAFE pin is done by SPI command 0x1D80 or 0xDD80.

5.2.3 SAFE safety path check

Figure 11 shows the connection for the safety path check at each start up.

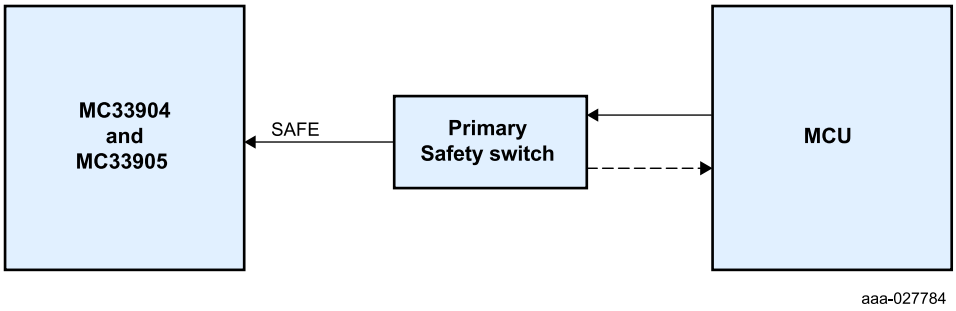

Figure 11. Safety path verification

A Safe activation can be requested by the SPI to check the hard connection between the Safe pin of the SBC and the safety switch. This request comes from the MCU, which must monitor the good activation and release of the safety switch through a sense path from the safety switch to the MCU.

This Safe activation can be done only in INIT mode.

Recommendation: It is recommended to verify the safety path at each startup of the system.

Rationale: To ensure the system is well in the safe state$_{system}$ when the SAFE is asserted low before starting the application.

- Internal register:
  In the MC33904 and MC33905, a write command can be sent by the MCU to request an SAFE activation
  SPE_MODE register, **sequence to follow**:
  - Read random code:
    - MOSI: 0001 0011 0000 0000 [Hex: 0x1300]
    - MISO report 16 bits, random code are bits (5-0). MISO= xxxx xxxx xxR5R4 R3R2R1R0
  - Write INIT mode = random code bits 5:4 not inverted and random code 3:0 inverted
    - MOSI: 0101 0010 01R5R4 Ri3Ri2Ri1Ri0 [Hex: 0x52HH] (RiX=random code inverted)

MISO = xxxx xxxx xxxx xxxx (don't care).

SPECIFIC MODE REGISTER

Table 4. Specific Mode Register, SPE_MODE

MOSI First Byte [15-8] [b_15 b_14] 01_001 [P/N]	MOSI Second Byte, bits 7-0							
	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
01 01_ 001 P	Sel_Mod[1]	Sel_Mod[0]	Rnd_C5b	Rnd_C4b	Rnd_C3b	Rnd_C2b	Rnd_C1b	Rnd_C0b
Default state	0	0	0		0	0	0	0
Condition for default	POR							

Bit	Description
b7, b6	**Sel_Mod[1], Sel_Mod[0]** - Mode selection: these 2 bits are used to select which mode the device will enter upon a SPI command.
00	RESET mode
01	INIT mode
10	FLASH mode
11	N/A
b5....b0	**[Rnd_C4b... Rnd_C0b]** - Random Code inverted, these 6 bits are the inverted bits obtained from the SPE-MODE Register read command.

5.3 Watchdog

A common mode may lead to a state where an MCU is unable to signal an internal failure. The likelihood of common mode failures affecting the functional safety of the system can be significantly reduced by using a system level timeout function, such as watchdog.

In general, the external watchdog covers common mode failures which are related to:

- Missing/wrong power
- Missing/wrong clocks
- Missing/wrong resets
- General destruction of internal components, such as latch-up at redundant input pads
- Errors in mode change, such as test, debug, or sleep/wake-up

Since these errors do not result in subtle output variations of the MCU, but typically in a complete failure, a temporal watchdog is sufficient. The watchdog function is required to be sufficiently independent to the SBC regarding clock generation, power supply, implementation or similar function.

The MC33904 and MC33905 act as a supervisor of the operation, and as a consequence, include a windowed watchdog (temporal and logical monitoring) which needs to be refreshed periodically by the MCU. It means the MC33904 and MC33905 watchdog function is in permanent communication with the MCU. As soon as there is no correct communication, after repetitive and defined tries, the SBC switches the system to safe $state_{system}$ within the FTTI. Thus, either the MCU or the SBC can switch the system to safe $state_{system}$.

Assumption: [SMR_17] It is the system integrator's responsibility to make sure the MCU periodically refreshes the MC33904 and MC33905 watchdog.[END]

Rationale: To cover situations, when the MCU is not able to signal a failure.

Implementation hint: Watchdog can be configured in different ways. It is recommended to use it in Window operation and at least in Enhanced 1 mode. The duration of the watchdog window is configurable to allow different MCU handshake strategies. The duty cycle of the window is fixed at 50 %. Therefore, the first half of the window is said closed and the second half of the window is said open. The watchdog must be refreshed in the middle of the open window. Enhanced 1 means that the MCU should first read a random code then compute this random code and send it back to SBC.

- Internal register:
  In the MC3390x, a register can be configured during initialization phase. The watchdog mode (Window operation and enhanced) should be configured during INIT phase only, while the watchdog window duration can be changed in both the INIT_FS and Normal_WD phases. Doing the change in normal operation allows the system integrator to configure the watchdog window duration on the fly (the new WD window duration is taken into account when the previous one is finished).

Table 5. Initialization Watchdog Registers, INIT W/D (note: register can be written only in INIT mode)

MOSI First Byte [15-8] [b_15 b_14] 0_0110 [P/N]	MOSI Second Byte, bits 7-0							
	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
01 00 _ 110 P	WD2INT	MCU_OC	OC-TIM	WD Safe	WD_spi[1]	WD_spi[0]	WD N/Win	Crank
Default state	0	1	0		0	0	1	0
Condition for default	POR							

Bit	Description
b3, b2	**WD_spi[1] WD_spi[0] -** Select the Watchdog (W/D) Operation
00	Simple Watchdog selection: W/D refresh done by a 8 bits or 16 bits SPI
01	Enhanced 1: Refresh is done using the Random Code, and by a single 16 bits.
10	Enhanced 2: Refresh is done using the Random Code, and by two 16 bits command.
11	Enhanced 4: Refresh is done using the Random Code, and by four 16 bits command.
b1	**WD N/Win -** Select the Watchdog (W/D) Window or Time out operation
0	Watchdog operation is TIMEOUT, W/D refresh can occur anytime in the period
1	Watchdog operation is WINDOW, W/D refresh must occur in the open window (second half of period)

Figure 12 shows the refresh slot allowed during WD refresh.

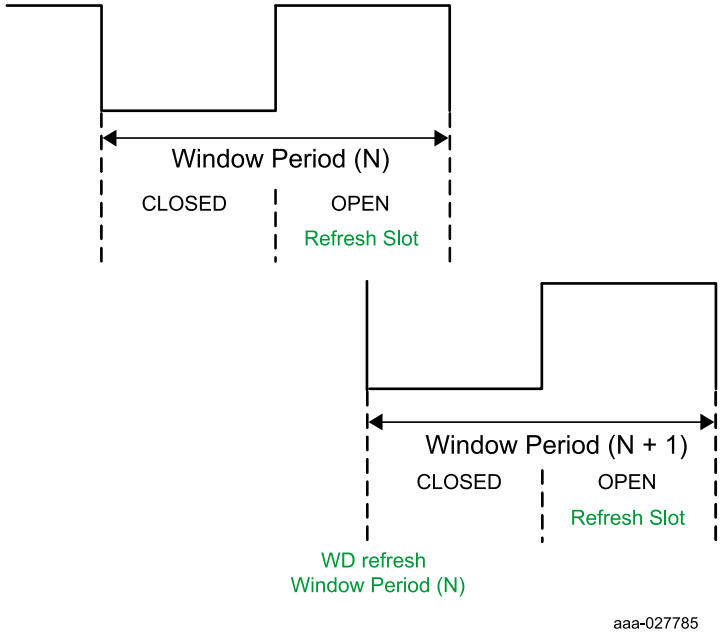

Figure 12. WD refresh slot

Several watchdog refresh operations can be selected: simple watchdog refresh or advance watchdog refresh. Advanced watchdog operation is recommended to improve coverage of potential MCU failure. Advanced watchdog consists to first read a code, then compute it and send it back to SBC. See Figure 13.

The enhanced 1 watchdog sequence is described below:

- The first time the device enters into normal mode (using 0x5A00 command), Random (RNDM) code must be read using the SPI command, 0x1B00. The device returns on MISO second byte the RNDM code. The full 16 bits MISO is called 0xXX**RD is the complement of the $\overline{\text{RD}}$ byte.**
- The refresh is command is 0x5A$\overline{\text{RD}}$. During each refresh command, the device will return on MISO, a new random code. This new random code must be inverted and send along with the next refresh command. It must be done in the open window, if the window operation is selected

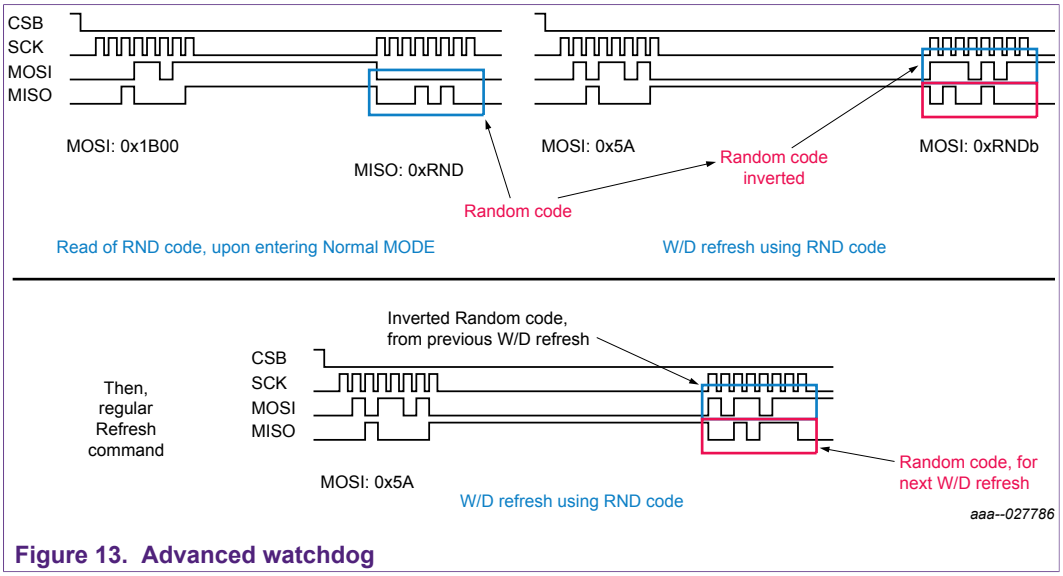

Figure 13. Advanced watchdog

Table 5 shows when a watchdog answer is considered as right or wrong.

Table 6. Watchdog error

		Window	
		Closed	Open
SPI	BAD key	WD_NOK	WD_NOK
	GOOD key	WD_NOK	WD_OK
	None (timeout)	No_issue	WD_NOK

5.4 Reset output - RSTB

RSTB is a dedicated active low signal integrated into the MC33904 and MC33905 to bring the MCU under RESET during an SBC internal fault or a fault reported by the system.

The duration of the reset is configurable during the initialization phase of the SBC. This duration is only used upon V_{DD} undervoltage detection.

Internal register:

In the MC3390x, a register can be configured only during the initialization phase to define the reset duration when it is asserted low in case of V_{DD} overvoltage only.

INIT REG register, **$V_{DD\ RST}$ [4:3]** bit (1.0 ms, 5 ms, 10 ms or 20 ms low level duration available). By default, the reset low duration time is set to 1.0 ms

Table 7. Initialization Regulator Registers, INIT REG (note: register can be written only in INIT mode)

MOSI First Byte [15-8] [b_15 b_14] 0_0101 [P/N]	MOSI Second Byte, bits 7-0							
	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
01 00 _ 101 P	I/Ox sync	V_{DDL} rst[1]	V_{DDL} rst[0]	V_{DD} rstD[1]	V_{DD} rstD[0]	V_{AUX}5/3	Cyclic on[1]	Cyclic on[0]
Default state	1	0	0	0	0	0	0	0
Condition for default	POR							

Bit	Description
b4, b3	V_{DD} rstD[1] V_{DD} rstD[0] - Select the Reset pin low lev duration, after V_{DD} rises above the V_{DD} under-voltage threshold
00	1.0 ms
01	5.0 ms
10	10 ms
11	20 ms

RSTB low pulse can also be requested by the SPI to check for a hard connection between the MCU reset pin and the MC3390x. This request comes from the MCU itself and is a software request. The goal is to verify the good RSTB hardware connection between the MCU and the MC3390x.

Internal register:

In the MC33904 and MC33905, a write command can be sent by the MCU to request an Reset activation.

SPE_MODE register, sequence to follow:

- Read random code:
  - MOSI: 0001 0011 0000 0000 [Hex: 0x1300]
  - MISO report 16 bits, random code are bits (5-0). MISO= xxxx xxxx xxR5R4 R3R2R1R0
- Write INIT mode + random code inverted
  - MOSI: 0101 0010 00Ri5Ri4 Ri3Ri2Ri1Ri0 [Hex: 0x52HH] (RiX=random code inverted)
  - MISO= xxxx xxxx xxxx xxxx (don't care)

The RSTB pin is bidirectional, therefore the MC3390x can bring the MCU under RESET and the MCU can maintain the RSTB low even if the MC3390x is ready to release it.

5.4.1 RSTB internal monitoring

RSTB pin is monitored to detect short-to-ground and short-to-high-voltage. Flags are reported in SAFE DEVICE FLAG register. An RSTB short-to-ground for at least 100 ms will activate the Safe state.

5.5 IO[1] - safe $state_{system}$ in case of V_{DD} overvoltage

The MC33904 and MC33905 have specific IO that can be configured as output to control safety circuitry in case of overvoltage detected on V_{DD}. The overvoltage should be at least 1.5 V above V_{DD} typical value to be detected, such as a short to Vsup. Then IO_1 will change from high to low output

Recommendation: It is recommended to configure the I/O_1 output pin to be asserted low when V_{DD} overvoltage is detected. And to wire the I/O_1 pin to the safe circuitry. [END]

Rationale: To put the application in safe $state_{system}$ in case of V_{DD} overvoltage.

Implementation hint: During initialization phase, set bit "I/O-1 on/off" to 1 in "INI LIN I/O register".

Internal register configuration:

In the MC33904 and MC33905, a register must be configured during initialization phase to activate the IO_1 on/off function.

INIT LIN I/O register, **I/O_1 on/off** and **I/0_1 out-en** bit must be enabled. By default, these bits are disabled.

Table 8. Initialization LIN and I/O registers, INIT LIN I/O (note: register can be written only in INIT mode)

MOSI First Byte [15-8] [b_15 b_14] 0_0111 [P/N]	MOSI Second Byte, bits 7-0							
	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
01 00 _ 111 P	I/O_1 ovoff	LIN_T1[1]	LIN_T1[0]	LIN_T0[1]	LIN_T0[0]	I/O_1 out-en	I/O_0 out-en	Cyc_Inv
Default state	0	0	0		0	0	0	0
Condition for default	POR							

Bit	Description
b7	**I/O_1 ovoff -** Select the deactivation of I/O_1 in case V_{DD} or V_{AUX} over-voltage condition is detected
0	Disable I/O_1 turn off.
1	Enable I/O_1 turn off, in case V_{DD} or V_{AUX} over-voltage condition is detected.
b2	**I/O_1 out-en**- Select the operation of the I/O_1 as output driver (high side, low side)
0	Disable high side and low side drivers of pin I/O_1. I/O_1 can only be used as input.
1	Enable high side and low side drivers of pin I/O_1. pin can be used as input and output driver.

Then in Normal mode, I/0_1 must be set as a high-side driver by enabled I/O_1[1:0] bits.

Table 9. I/O Register, I/O

MOSI First byte [15-8] [b_15 b_14] 10_001 [P/N]	MOSI Second Byte, bits 7-0							
	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
01 10_ 001P	I/O_3 [1]	I/O_3 [0]	I/O_2 [1]	I/O_2 [0]	I/O_1 [1]	I/O_1 [0]	I/O_0 [1]	I/O_0 [0]
Default state	0	0	0	0	0	0	0	0
Condition for default	POR							

Bits	Description
b3 b2	I/O_1 [1], I/O_1 [0] - I/O_1 pin operation
00	I/O_1 driver disable, Wake-up capability disable
01	I/O_1 driver disable, Wake-up capability enable.
10	I/O_1 Low Side driver enable.
11	I/O_1 High Side driver enable.

Figure 14 shows an example of an application using IO_1 to control safe circuitry.

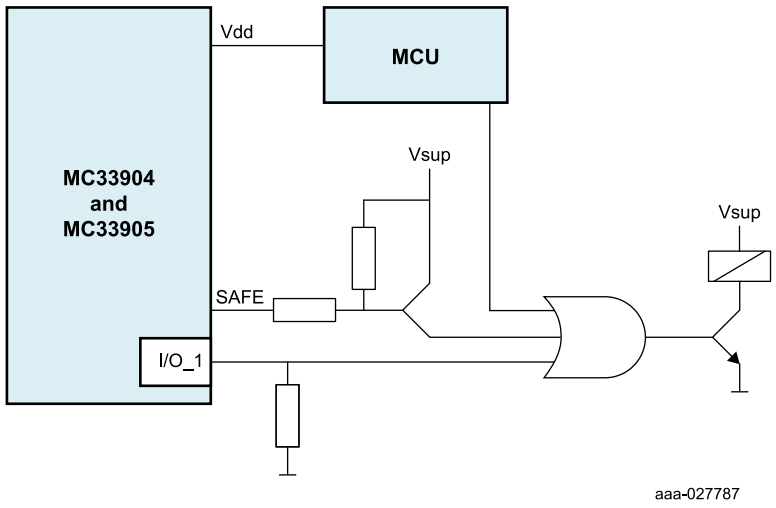

Figure 14. IO_1 connection to Safe circuitry

As for SAFE output, ensure that the good activation of the I/O_1 is recommended after POR. It can be done by setting the I/O_1 output as a low-side driver. Check that the output level is zero or that the system is in safe state.

5.6 Debug mode

A debug mode is available on the device to help the system engineer to develop software. Refer to the MC33904 and MC33905 data sheet (DEBUG chapter) to learn how to enter and exit debug mode.

In debug mode, the watchdog window is fully open and no watchdog refresh is required. This allows an easy debug of the hardware and software routines, such as SPI commands.

Assumption: [SMR_18] It is the system integrator's responsibility to make sure Device is not in DEBUG mode after system startup. [END]

Rationale: To ensure the product is not working in debug mode and by consequence is able to assert the safety outputs RSTB and/or SAFE low, in case of a watchdog refresh error.

Implementation hint: Two SPI commands can be sent to be sure the device is not in Debug mode, or at least deactivate it. Commands 0x1D00 and 0xDD00.

Table 10. Device Modes

Global commands and effects								
Read device current mode, Leave debug mode. Keep SAFE pin as is. MOSI in hexadecimal: 1D 00	MOSI	**bits 15 to14**	**bits 13 to 9**	**bit 8**	**bit 7**	**bits 6 to 0**		
		00	01 110	1	0	000 0000		
	MISO	**bit 15 to 8**		**bit 7 to 3**		**bit 2 to 0**		
		Fix Status		Device current mode		Random code		
Read device current mode, Leave debug mode. Keep SAFE pin as is. MOSI in hexadecimal: DD 00 MISO reports Debug and SAFE state (bits 1,0)	MOSI	**bits 15 to 14**	**bits 13 to 9**	**bit 8**	**bit 7**	**bits 6 to 0**		
		11	01 110	1	0	000 0000		
	MISO	**bit 15 to 8**		**bit 7 to 3**		**bit 2**	**bit 1**	**bit 0**
		Fix Status		Device current mode		X	SAFE	DEBUG

5.7 Safe state

MC33904 and MC33905 have four different safe states available. Safe mode is selected by connecting resistor to DEBUG pin. This hardware selection can be overwritten by SPI command. Below are the four safe modes available:

Assumption: [SMR_19] It is the system integrator's responsibility to make sure the device is in the right safe state after system startup. [END]

Rationale: To ensure the product will go in the desired safe state in case of sate output activation.

Implementation hint: One SPI command can be sent to read and overwrite the Safe state detection made by a resistor in case of a wrong detection.

Bits b2,1 and 0 allow the following operation:

First, check that the resistor device has been detected at the Debug pin. If the resistor is different, bit 5 (Debug resistor) is set in Safe register (refer to device flag table in datasheet).

Second, over write the resistor decoded by device, to set the SAFE mode operation by SPI. Once this function is selected by bit 2 =1, this selection has higher priority than "hardware", and device will behave according to b2,b1 and b0 setting

Table 11. Initialization Miscellaneous Functions, INIT MISC (Note: Register can be written only in INIT mode)

MOSI First Byte [15-8] [b_15 b_14] 0_1000 [P/N]	MOSI Second Byte, bits 7-0							
	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
01 01_ 000 P	LPM w RND	SPI parity	INT pulse	INT width	INT flash	Dbg Res[2]	Dbg Res[1]	Dbg Res[0]
Default state	0	0	0		0	0	0	0
Condition for default	POR							

Bit	Description
b2, b1, b0	**Dbg Res[2], Dbg Res[1], Dbg Res[0] -** Allow verification of the external resistor connected at DBG pin. Ref to parametric table for resistor range value.
0xx	Function disable
100	100 verification enable: resistor at DBG pin is typ 68 kΩ (RB3) - Selection of SAFE mode B3
101	101 verification enable: resistor at DBG pin is typ 33 kΩ (RB2 - Selection of SAFE mode B2
110	110 verification enable: resistor at DBG pin is typ 15 kΩ (RB1) - Selection of SAFE mode B1
111	111 verification enable: resistor at DBG pin is typ 0 kΩ (RA) - Selection of SAFE mode A

5.8 Physical layers

5.8.1 LIN mode during RSTB assertion

When RSTB is asserted low, the LIN physical layer is automatically disabled to avoid miscommunication. When RSTB is released and the device is in Normal mode, the LIN physical layer is automatically enabled. The configuration of the LIN layer depends on the LIN mode [1:0] bits.

5.8.2 CAN mode during RSTB assertion

When RSTB is asserted low, the CAN physical layer is automatically disabled to avoid miscommunication. When RSTB is released, the CAN physical layer is automatically enabled. The configuration of the CAN layer depends on the CAN mod[1:0] bits.

6 Startup sequence

After power up, the device releases the reset after approximately 1.5 ms. When the reset is released, V_{DD} is on and the fail-safe SAFE pin is asserted low. At this stage, the device is in INIT phase. The device is ready to be configured.

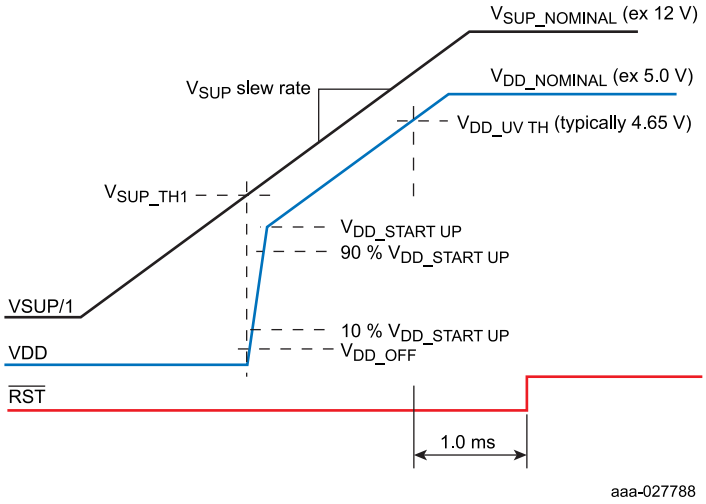

Figure 15. Start-up sequence diagram

When the reset is released, the MCU has an open window of 256 ms to configure the device and to send the first good WD refresh. If the first good WD is not refreshed within 256 ms, a reset is sent to the MCU.

6.1 INIT phase

During this phase, all the initialization registers can be accessed and configured. Refer to the MC3390x data sheet to know which registers can be configured during the INIT phase only.

1. Verify
   - Verify BATFAIL bit status and clear it if bit is set
   - Verify debug mode is not activated
     - Leave Debug mode if it is activated
     - Verify safe state configuration
2. Configure
   - Configure I/O_1 as an output, HS driver
   - Configure I/O_1 to be deactivated in case of V_{DD} overvoltage
   - Configure the WD window period and the advance WD mode
3. Execute
   - Close the INIT phase
   - Clear all the flags by reading all diag registers
   - Release SAFE pin if asserted (no PORb). After POR, the MCU must maintain its own safety path to low, because the safe pin is not asserted at startup.
   - Perform a safety path check for both SAFE

The MC33904 or MC33905 is now ready. If everything is ok for the MCU, it can release its own safety path and the ECU starts.

7 Acronyms and abbreviations

A short list of acronyms and abbreviations used in this document is summarized for completeness:

Table 12. Acronyms and abbreviations

Term	Meaning
ADC	Analog-to-digital converter
CCF	Common cause failure
CF	Cascading failure
CMF	Common mode failure
DPF	Dual-point fault
FMEDA	Failure modes, effects and diagnostic analysis
FTTI	Single-point fault tolerant time interval
GPIO	General purpose I/O
MPFDI	Multiple-point fault detection Interval
LF	Latent fault
MCU	Microcontroller unit
MPF	Multiple-point fault
OV	Overvoltage
RF	Residual fault
SBC	System basis chip
SF	Safe fault
SPF	Single-point fault
UV	Undervoltage

7.1 Safety tags

Table 13. Safety tags

Tag	Assumption
[SMR_01]	It is assumed the MC33904 and MC33905 are used in 12-volt automotive applications for which the battery voltage (pin VSUP1, VSUP,2, and VSENSE) never exceeds the maximum ratings of theMC33904 and MC33905 (28 V). Above this voltage, the MC33904 and MC33905 run the risk of being destroyed and the safety requirements are no longer satisfied.
[SMR_02]	It is assumed the MC33904 and MC33905 are used in applications for which the fault tolerant time interval is ≥ 256 ms. A shorter fault tolerant time interval must be deeply analyzed. This time interval can be reduced to 100 ms
[SMR_03]	It is assumed the MC33904 and MC33905 are used in applications for which the mission profile is equivalent to or less aggressive, see Table 1.
[SMR_04]	It is assumed that when the multiple point fault time interval is ≤ 12 hours, the driving cycle is ≤ 12 hours.
[SMR_05]	It is assumed the normal operating range of the MC33904 and MC33905 is fulfilled by the compliance to the MC33904 and MC33905 data sheet.
[SMR_06]	To avoid systematic errors during system integration, it is the system integrator's responsibility to follow NXP recommendations as described in the MC33904 and MC33905 data sheet and application note. Both documents are available at www.nxp.com.
[SMR_07]	It is the system integrator's responsibility to report all field failures of a device to the silicon supplier.

Tag	Assumption
[SMR_08]	It is the system integrator's responsibility to ensure the system transitions itself to a safe $state_{system}$ when the MC33904 and MC33905 explicitly indicates an error via its Fail-safe outputs (SAFE)
[SMR_09]	It is the system integrator's responsibility to ensure the system transitions itself to a safe $state_{system}$ when the MC33904 and MC33905 are completely unpowered.
[SMR_10]	It is assumed single-point and latent fault diagnostic measures complete operations (including fault reaction) in a time shorter than the respective FTTI when the safety function is enabled.
[SMR_11]	t is assumed simultaneous pin disconnections, such as a pin lift on the PCB, are restricted to 1 during pin FMEA and FMEDA analysis.
[SMR_12]	It is assumed the thermal connection of the exposed pad to the PCB is always ensured due to its large size.
[SMR_13]	Short-circuit between PCB tracks is not considered.
[SMR_14]	External component disconnection is not considered.
[SMR_15]	An output in high-impedance is not considered safe at the system level. It is the system integrator's responsibility to make sure external components connected to SAFE are available to bring the safety critical outputs to a known level during operation.
[SMR_16]	It is the system integrator's responsibility to ensure opening the safety switch in a system must not be driven by the SAFE only, but also by the MCU or I/O_1.
[SMR_17]	It is the system integrator's responsibility to make sure the MCU periodically refreshes the MC33904 and MC33905 watchdog.
[SMR_18]	It is the system integrator's responsibility to make sure the device is not in DEBUG mode after system startup.
[SMR_19]	It is the system integrator's responsibility to make sure the device is the right safe state after system startup.
If any of these safety manual requirements is not respected, the impact in the FMEDA metrics must be verified.	

8 Revision history

Revision	Date	Description of changes
1.0	201700921	Initial release

9 Legal information

9.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

9.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Suitability for use in automotive applications — This NXP Semiconductors product has been qualified for use in automotive applications. Unless otherwise agreed in writing, the product is not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

9.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 21 September 2017
Document identifier: AN12048